04336048 **Image available**
MULTI-ADDRESS COMMUNICATION SYSTEM

PUB. NO.: 05-327748 [JP 5327748 A]
PUBLISHED: December 10, 1993 (19931210)
INVENTOR(s): TORII NAOYA
AKIYAMA RYOTA
HASEBE TAKAYUKI
APPLICANT(s): FUJITSU LTD [000522] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-134876 [JP 92134876]
FILED: May 27, 1992 (19920527)
INTL CLASS: [5] H04L-012/44; G06F-013/00; G09C-001/00; H04L-009/06; H04L-009/14
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.2 (INFORMATION PROCESSING -- Memory Units)
JOURNAL: Section: E, Section No. 1522, Vol. 18, No. 148, Pg. 150, March 11, 1994 (19940311)

ABSTRACT

PURPOSE: To shorten the key distributing time and to decrease the number of storage keys by multi-addressing the ciphering data to a group of user terminals from a center via a star line network.

CONSTITUTION: A means 16 of a center 10 produces a tree which covers the center 10 through each user terminal 12. Meanwhile a means 18 of the center 10 assigns the proper numbers and the master keys to all nodes included in the tree. A means 20 defines a node proper number and a master key to each terminal 12, and a means 22 ciphers the session key with the master key of the node shown by the designated proper number. Then the means 24 ciphers the data to be multi-addressed to the terminals of the lower ranks than a node layer by means of the session key.
?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報(A)**　(11)特許出願公開番号

特開平5－327748

(43)公開日　平成５年(1993)12月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/44				
Ｇ０６Ｆ　13/00	３５１　Ｚ	7368－5Ｂ		
Ｇ０９Ｃ　1/00		9194－5Ｌ		
		8529－5Ｋ	Ｈ０４Ｌ　11／00　３４０	
		7117－5Ｋ	9／02　Ｚ	

審査請求　未請求　請求項の数７(全 30 頁)　最終頁に続く

(21)出願番号　特願平4－134876

(22)出願日　平成４年(1992)５月27日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　島居　直哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

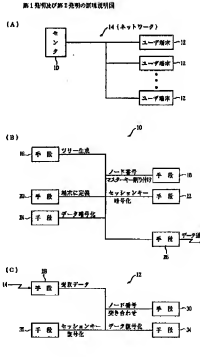
(74)代理人　弁理士　伊藤　儀一郎

(54)【発明の名称】　同報通信システム

(57)【要約】

【目的】　本発明は、センタからユーザ端末グループへ暗号化データがスター状のネットワークを介して同報されるシステムに関し、キー配送時間の短縮，保管キーの減少が可能となる同報通信システムの提供を目的とする。

【構成】　センタ１０は、各ユーザ端末１２に至るツリーの生成手段１６と、ツリー上に存在の全ノードへ固有番号とマスタキーを割り付ける手段１８と、各ユーザ端末１２にノード固有番号とマスタキーを定義する手段２０と、指定の固有番号が示すノードのマスタキーでセッションキーを暗号化する手段２２と、該ノードのレイヤより下位側の端末グループへ同報送信すべきデータをセッションキーで暗号化する手段２４と、指定のノード固有番号と暗号化されたセッションキー及びデータとをネットワーク１４へ送出する手段２６と、を有する。



1

【特許請求の範囲】

【請求項1】　単一のセンタ（10）と多数のユーザ端末（12）とがスター状のネットワーク（14）で結ばれ、センタ（10）からユーザ端末（12）のグループへ暗号化されたデータがネットワーク（14）を介して同報される同報通信システムにおいて、

センタ（10）は、

センタ（10）と全てのユーザ端末（12）とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段（16）と、

センタ（10）から各ユーザ端末（12）へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段（18）と、

各ユーザ端末（12）についてセンタ（10）から自端末（12）に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（20）と、

指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段（22）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（12）のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段（24）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（14）へ送出する手段（26）と、

を有し、

各ユーザ端末（12）は、

センタ（10）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（14）を介してセンタ（10）から受け取る手段（28）と、

手段（28）がネットワーク（14）から受け取ったノード固有番号とセンタ（10）側から予め秘密配布された自端末（12）のノード固有番号とを突き合わせて自端末（12）が同報送信先となる端末グループのメンバであるか否かを判定する手段（30）と、

自端末（12）が同報送信先となる端末グループのメンバであるときに手段（28）がネットワーク（14）から受け取ったセッションキーデータをセンタ（10）側から予め秘密配布された自端末（12）のマスタキーデータで復号する手段（32）と、

手段（28）がネットワーク（14）から受け取ったデータを復号されたセッションキーデータで復号する手段（34）と、

を有する、ことを特徴とした同報通信システム。

【請求項2】　単一のセンタ（10）と多数のユーザ端末（12）とがスター状のネットワーク（14）で結ばれ、センタ（10）からユーザ端末（12）のグループへ暗号化されたデータがネットワーク（14）を介して

2

同報される同報通信システムにおいて、

センタ（10）は、

センタ（10）と全てのユーザ端末（12）とが最上位のレイヤと最下位のレイヤとに各々配置されたバイナリツリーを生成する手段（16）と、

センタ（10）から各ユーザ端末（12）へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段（18）と、

各ユーザ端末（12）についてセンタ（10）から自端末（12）に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータを定義する手段（20）と、

指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段（22）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（12）のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段（24）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（14）へ送出する手段（26）と、

を有し、

各ユーザ端末（12）は、

センタ（10）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（14）を介してセンタ（10）から受け取る手段（28）と、

手段（28）がネットワーク（14）から受け取ったノード固有番号とセンタ（10）側から予め秘密配布された自端末（12）のノード固有番号とを突き合わせて自端末（12）が同報送信先となる端末グループのメンバであるか否かを判定する手段（30）と、

自端末（12）が同報送信先となる端末グループのメンバであるときに手段（28）がネットワーク（14）から受け取ったセッションキーデータをセンタ（10）側から予め秘密配布された自端末（12）のマスタキーデータで復号する手段（32）と、

手段（28）がネットワーク（14）から受け取ったデータを復号されたセッションキーデータで復号する手段（34）と、

を有する、

ことを特徴とした同報通信システム。

【請求項3】　単一のセンタ（10）と多数のユーザ端末（12）とがスター状のネットワーク（14）で結ばれ、センタ（10）からユーザ端末（12）のグループへ暗号化されたデータがネットワーク（14）を介して同報される同報通信システムにおいて、

センタ（10）は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意す

る手段（４０）と、
センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段（４２）と、
手段（４０）が予め用意した最小公倍数と互いに素となる数のマスタキーデータと固有の番号とをセンタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した各ノードへ割り付ける手段（４４）と、
各ユーザ端末（１２）についてセンタ（１０）から自端末（１２）へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（４６）と、
手段（４０）が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段（４０）が予め用意した最小公倍数と手段（４０）が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末（１２）について作成する手段（４８）と、
指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段（４０）が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段（５０）と、
作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段（５２）と、
指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（１２）へ同報すべきデータをセッションキーデータで暗号化する手段（５４）と、
指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（１４）へ送出する手段（５６）と、
を有し、
各ユーザ端末（１２）は、
センタ（１０）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（１４）を介して受け取る手段（５８）と、
手段（５８）がネットワーク（１４）から受け取ったノード固有番号とセンタ（１０）側から予め配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバであるか否かを判定する手段（６０）と、
自端末（１２）が同報送信先となる端末グループのメンバであるときに自端末（１２）のパスワードとセンタ（１０）側から予め配布された自端末（１２）のマスタキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段（６２）と、
手段（５８）がネットワーク（１４）から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段（６４）と、
手段（５８）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段

（６６）と、
を有する、
ことを特徴とした同報通信システム。
【請求項４】　単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して同報される同報通信システムにおいて、
センタ（１０）は、
十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段（４０）と、
センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段（４２）と、
手段（４０）が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した各ノードへ割り付ける手段（４４）と、
各ユーザ端末（１２）についてセンタ（１０）から自端末（１２）へ至るツリー中の経路上に存在した全ノードのマスタキーデータと固有番号とを定義する手段（４６）と、
手段（４０）が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段（４０）が予め用意した最小公倍数と手段（４０）が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末（１２）について作成する手段（４８）と、
指定された固有番号に対応したレイヤよりセンタ（１０）側に配置された各ノードのマスタキーデータと手段（４０）が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段（５０）と、
作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段（５２）と、
指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（１２）へ同報すべきデータをセッションキーデータで暗号化する手段（５４）と、
指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（１４）へ送出する手段（５６）と、
を有し、
各ユーザ端末（１２）は、
センタ（１０）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（１４）から受け取る手段（５８）と、
手段（５８）がネットワーク（１４）から受け取ったノード固有番号とセンタ（１０）側から予め配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバであ

るか否かを判定する手段（６０）と、
自端末（１２）が同報送信先となる端末グループのメンバであるときに自端末（１２）のパスワードとセンタ（１０）側から予め配布された自端末（１２）のマスタキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段（６２）と、
手段（５８）がネットワーク（１４）から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段（６４）と、
手段（５８）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段（６６）と、
を有する、
ことを特徴とした同報通信システム。
【請求項５】　単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して同報される同報通信システムにおいて、
センタ（１０）は、
十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段（７０）と、
センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段（７２）と、
手段（７０）が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した各ノードへ割り付ける手段（７４）と、
各ユーザ端末（１２）についてセンタ（１０）から自端末（１２）へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（７６）と、
上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末（１２）についてグループキーデータを定義する手段（７８）と、
手段（７０）が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段（７０）が予め用意した最小公倍数と手段（７０）が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末（１２）について作成する手段（８０）と、
指定された固有番号に対応するノード及び該ノード上下位側のレイヤに配置された各ノードのマスタキーデータと手段（７０）が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段（８２）と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段（８４）と、
指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（１２）へ同報すべきデータをセッションキーデータで暗号化する手段（８６）と、
指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（１４）へ送出する手段（８８）と、
を有し、
各ユーザ端末（１２）は、
センタ（１０）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（１４）を介して受け取る手段（９０）と、
手段（９０）がネットワーク（１４）から受け取ったノード固有番号とセンタ（１０）側から予め配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバであるか否かを判定する手段（９２）と、
自端末（１２）が同報送信先となる端末グループのメンバであるときに自端末（１２）のパスワードとセンタ（１０）側から予め配布された自端末（１２）のマスタキーデータ，キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段（９４）と、
手段（９０）がネットワーク（１４）から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段（９６）と、
手段（９０）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段（９８）と、
を有する、
ことを特徴とした同報通信システム。
【請求項６】　単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して同報される同報通信システムにおいて、
センタ（１０）は、
十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段（７０）と、
センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたバイナリツリーを生成する手段（７２）と、
手段（７０）が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した各ノードへ割り付ける手段（７４）と、

7

各ユーザ端末（12）についてセンタ（10）から自端末（12）へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（76）と、

上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末（12）についてグループキーデータを定義する手段（78）と、

手段（70）が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段（70）が予め用意した最小公倍数と手段（70）が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末（12）について作成する手段（80）と、

指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段（70）が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段（82）と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段（84）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（12）へ同報すべきデータをセッションキーデータで暗号化する手段（86）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（14）へ送出する手段（88）と、

を有し、

各ユーザ端末（12）は、

センタ（10）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（14）を介して受け取る手段（90）と、

手段（90）がネットワーク（14）から受け取ったノード固有番号とセンタ（10）側から予め配布された自端末（12）のノード固有番号とを突き合わせて自端末（12）が同報送信先となる端末グループのメンバであるか否かを判定する手段（92）と、

自端末（12）が同報送信先となる端末グループのメンバであるときに自端末（12）のパスワードとセンタ（10）側から予め配布された自端末（12）のマスタキーデータ，キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段（94）と、

手段（90）がネットワーク（14）から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段（96）と、

手段（90）がネットワーク（14）から受け取ったデータを復号されたセッションキーデータで復号する手段（98）と、

を有する、

ことを特徴とした同報通信システム。

8

【請求項7】　単一のセンタ（10）と多数のユーザ端末（12）とがスター状のネットワーク（14）で結ばれ、センタ（10）からユーザ端末（12）のグループへ暗号化されたデータがネットワーク（14）を介して同報される同報通信システムにおいて、

センタ（10）は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段（70）と、

センタ（10）と全てのユーザ端末（12）とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段（72）と、

手段（70）が予め用意した最小公倍数と互いに素となる数のマスタキーデータと固有の番号とをセンタ（10）から各ユーザ端末（12）へ至るツリー中の経路上に存在した各ノードへ割り付ける手段（74）と、

各ユーザ端末（12）についてセンタ（10）から自端末（12）へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（76）と、

上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末（12）についてグループキーデータを定義する手段（78）と、

手段（70）が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段（70）が予め用意した最小公倍数と手段（70）が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末（12）について作成する手段（80）と、

指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段（70）が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段（82）と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段（84）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（12）へ同報すべきデータをセッションキーデータで暗号化する手段（86）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（14）へ送出する手段（88）と、

を有し、

各ユーザ端末（12）は、

センタ（10）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（14）を介して受け取る手段（90）と、

手段（90）がネットワーク（14）から受け取ったノ

9

ード固有番号とセンタ（１０）側から予め配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバであるか否かを判定する手段（９２）と、

自端末（１２）が同報送信先となる端末グループのメンバであるときに自端末（１２）のパスワードとセンタ（１０）側から予め配布された自端末（１２）のマスタキーデータ，キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段（９４）と、

手段（９０）がネットワーク（１４）から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段（９６）と、

手段（９０）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段（９８）と、

を有する、

ことを特徴とした同報通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、単一のセンタからユーザ端末のグループ暗号化されたデータがスター状のネットワークを介して同報される同報通信システムに関する。

【０００２】衛星を介してデータを送信する場合で、契約などにより限られたユーザの端末だけにそのデータをセンタから同報するときには、他の端末で同報のデータを傍受されないように、このデータが暗号化される。

【０００３】

【従来の技術】センタにホストコンピュータが有線回線を介して接続され、各ユーザ端末の要求に応じ、センタとユーザの端末との間で衛星回線を介してデータの送受信が行なわれる。

【０００４】そのデータ通信はセンタで一元的に管理され、多くの場合、データ通信に際し、個々のユーザ回線を多重化して送受信を行なう個別送信モードと複数のユーザをメンバとするグループにセンタより暗号化されたデータを同報する同報モードとのいずれかが選択される。

【０００５】ここで同報モードが選択されると、グループ暗号通信のためのセッションキーがセンタで生成され、また、ユーザ端末毎にセッション毎に配送用のマスタキーが定められる。そして、セッションキーはマスタキーで暗号化されて各ユーザ端末へ配送され（暗号化セッションキー）、暗号化された同報データの復元に各ユーザ端末で利用される。

【０００６】

【発明が解決しようとする課題】同報先となる端末グループを構成するユーザ端末の全てに、該当の暗号化セッションキーを配送する場合、グループメンバ（ユーザ端

10

末）の数とともにキー配送の所要時間が増加する。

【０００７】そのユーザ端末の総数は一般に数百万に達し、同報先となる端末グループのメンバ数も極めて多いものとなる。したがって、セッション毎キーの配送に長時間を要する。

【０００８】また、全てのマスタキーを予め配布して各ユーザ端末で管理する方式の場合には、センタ局側で管理すべきグループキーがユーザ端末側のものを含めて２＊＊ｔ－１（ｔはユーザ端末数を意味し、ａ＊＊ｂはａのｂ乗を意味する）本となり、ユーザ端末側においても２＊＊（ｔ－１）－１本のマスタキーを保管することが必要となるので、ユーザ端末数が数百万となることから、キー保管のデータ量が膨大なものとなる。

【０００９】本発明は上記従来の事情に鑑みてなされたものであり、その目的は、キー配送時間の短縮，保管キーの減少が可能となる同報通信システムを提供することにある。

【００１０】

【課題を解決するための手段】

／＊　第１発明　＊／

図１（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループ暗号化されたデータがネットワーク１４を介して同報される。

【００１１】この図１（Ａ）のセンタ１０は、同図（Ｂ）において、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段１６と、センタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段１８と、各ユーザ端末１２についてセンタ１０から自端末１２に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータを定義する手段２０と、指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段２２と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段２４と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段２６と、を有する。

【００１２】また図１（Ａ）の各ユーザ端末１２は、同図（Ｃ）において、センタ１０から送出されたノード固有番号とセッションキーデータとデータとをネットワーク１４を介してセンタ１０から受け取る手段２８と、手段２８がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め秘密配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段３０と、自端末１２が同報送信先となる端末グル

11

プのメンバであるときに手段２８がネットワーク１４から受け取ったセッションキーデータをセンタ１０側から予め秘密配布された自端末１２のマスタキーデータで復号する手段３２と、手段２８がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段３４と、を有する。

【００１３】／＊　第２発明　＊／

図１（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

【００１４】この図１（Ａ）のセンタ１０は、同図（Ｂ）において、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置されたバイナリツリーを生成する手段１６と、センタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段１８と、各ユーザ端末１２についてセンタ１０から自端末１２に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータを定義する手段２０と、指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段２２と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段２４と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段２６と、を有する。

【００１５】また図１（Ａ）の各ユーザ端末１２は、同図（Ｃ）において、センタ１０から送出されたノード固有番号とセッションキーデータとデータとをネットワーク１４を介してセンタ１０から受け取る手段２８と、手段２８がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め秘密配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段３０と、自端末１２が同報送信先となる端末グループのメンバであるときに手段２８がネットワーク１４から受け取ったセッションキーデータをセンタ１０側から予め秘密配布された自端末１２のマスタキーデータで復号する手段３２と、手段２８がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段３４と、を有する。

【００１６】／＊　第３発明　＊／

図２（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

【００１７】この図２（Ａ）のセンタ１０は、同図（Ｂ）において、十分に大きな一対の素数と両素数の乗

12

算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段４０と、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段４２と、手段４０が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付ける手段４４と、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段４６と、手段４０が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段４０が予め用意した最小公倍数と手段４０が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する手段４８と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段４０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段５０と、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段５２と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータをセッションキーデータで暗号化する手段５４と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段５６と、を有する。

【００１８】また図２（Ａ）の各ユーザ端末１２は、同図（Ｃ）において、センタ１０が送出したノード固有番号とセッションキーデータとデータとをネットワーク１４から受け取る手段５８と、手段５８がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段６０と、自端末１２が同報送信先となる端末グループのメンバであるときに自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段６２と、手段５８がネットワーク１４から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段６４と、手段５８がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段６６と、を有する。

【００１９】／＊　第４発明　＊／

図２（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

【００２０】この図２（Ａ）のセンタ１０は、同図

13

(B) において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段４０と、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段４２と、手段４０が予め用意した最小公倍数と互いに素となる数のマスタキーデータと固有の番号とをセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付ける手段４４と、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードのマスタキーデータと固有番号とを定義する手段４６と、手段４０が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段４０が予め用意した最小公倍数と手段４０が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する手段４８と、指定された固有番号に対応したノード及び該ノード下位側のレイヤに配置された各ノードのマスタキーデータと手段４０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段５０と、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段５２と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータをセッションキーデータで暗号化する手段５４と、指定された ノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段５６と、を有する。

【０００１】また図２ (A) の各ユーザ端末１２は、同図 (C) において、センタ１０が送出したノード固有番号とセッションキーデータとデータとをネットワーク１４から受け取る手段５８と、手段５８がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段６０と、自端末１２が同報送信先となる端末グループのメンバであるときに自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段６２と、手段５８がネットワーク１４から受け取ったセッションキーデータを生成された キー暗号化キーデータで復号する手段６４と、手段５８がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段６６と、を有する。

【０００２】／＊　第５発明　＊／

図３ (A) において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

14

【０００３】この図３ (A) のセンタ１０は、同図 (B) において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段７０と、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段７２と、手段７０が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付ける手段７４と、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段７６と、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末１２についてグループキーデータを定義する手段７８と、手段７０が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段７０が予め用意した最小公倍数と手段７０が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する手段８０と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段７０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段８２と、を有する。

【００２４】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段８４と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータをセッションキーデータで暗号化する手段８６と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段８８と、を有する。

【００２５】また図３ (A) の各ユーザ端末１２は、同図 (C) において、センタ１０が送出したノード固有番号とセッションキーデータとデータとをネットワーク１４から受け取る手段９０と、手段９０がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段９２と、自端末１２が同報送信先となる端末グループのメンバであるときに自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段９４と、手段９０がネットワーク１４から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段９６と、手段９０がネットワ

15

ーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段９８と、を有する。

【００２６】／＊　第６発明　＊／

図３（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

【００２７】この図３（Ａ）のセンタ１０は、同図（Ｂ）において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段７０と、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数が上位側となるレイヤのノード数を越えて設定されたバイナリツリーを生成する手段７２と、手段７０が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付ける手段７４と、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードのマスタキーデータと固有番号とを定義する手段７６と、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末１２についてグループキーデータを定義する手段７８と、手段７０が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段７０が予め用意した最小公倍数と手段７０が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する手段８０と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段７０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段８２と、を有する。

【００２８】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段８４と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータをセッションキーデータで暗号化する手段８６と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段８８と、を有する。

【００２９】また図３（Ａ）の各ユーザ端末１２は、同図（Ｃ）において、センタ１０が送出したノード固有番号とセッションキーデータとデータとをネットワーク１４から受け取る手段９０と、手段９０がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段９２と、自端末１２が同

16

報送信先となる端末グループのメンバであるときに自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段９４と、手段９０がネットワーク１４から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段９６と、手段９０がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段９８と、を有する。

【００３０】／＊　第７発明　＊／

図３（Ａ）において、単一のセンタ１０と多数のユーザ端末１２とがスター状のネットワーク１４で結ばれ、センタ１０からユーザ端末１２のグループへ暗号化されたデータがネットワーク１４を介して同報される。

【００３１】この図３（Ａ）のセンタ１０は、同図（Ｂ）において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段７０と、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段７２と、手段７０が予め用意した最小公倍数と互いに素となる数のマスタキーデータと固有の番号とをセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付ける手段７４と、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段７６と、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末１２についてグループキーデータを定義する手段７８と、手段７０が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段７０が予め用意した最小公倍数と手段７０が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する手段８０と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段７０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段８２と、を有する。

【００３２】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段８４と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータをセッションキーデータで暗号化する手段８６と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク１４へ送出する手段８８と、を有する。

【００３３】また図３（Ａ）の各ユーザ端末１２は、同

図（C）において、センタ１０が送出したノード固有番号とセッションキーデータとデータとをネットワーク１４から受け取る手段９０と、手段９０がネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合わせて自端末１２が同報送信先となる端末グループのメンバであるか否かを判定する手段９２と、自端末１２が同報送信先となる端末グループのメンバであるときに自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ，キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段９４と、手段９０がネットワーク１４から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段９６と、手段９０がネットワーク１４から受け取ったデータを復号されたセッションキーデータで復号する手段９８と、を有する。

【００３４】

【作用】

／＊　第１発明　第２発明　＊／

ユーザ端末１２の総数が与えられることにより、グループキー配送用のツリーが作成される。

【００３５】このツリーはセンタ１０が配置されたルートの最上位レイヤから２枝またはそれ以上に分岐しながら伸長し、レイヤ（ｉ）は枝分岐毎に０，１，２，・・・と下位側へ増加し、各レイヤにおけるノード（ｊ）の数はその上位側レイヤからの分岐倍となり、ツリーは最下位レイヤのノード数がユーザ端末１２の総数に達したときに伸長を停止する。

【００３６】図４においてはユーザ端末１２の総数が８とされたバイナリツリーが示されており、レイヤが０から３まで増加してユーザ端末１２の総数と対応したノード数が７へ達したときに、ツリーがその伸長を停止する。

【００３７】さらに、センタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した全てのノードに、固有の番号ＮｉｊとマスタキーデータＫｉｊとが割り付けられる。

【００３８】図４においては、固有番号Ｎ００，Ｎ１０，Ｎ１１，Ｎ２０，Ｎ２１，Ｎ２２，Ｎ２３，Ｎ３０，Ｎ３１，Ｎ３２，Ｎ３３，Ｎ３４，Ｎ３５，Ｎ３６，Ｎ３７とマスタキーデータＫ００，Ｋ１０，Ｋ１１，Ｋ２０，Ｋ２１，Ｋ２２，Ｋ２３，Ｋ３０，Ｋ３１，Ｋ３２，Ｋ３３，Ｋ３４，Ｋ３５，Ｋ３６，Ｋ３７とが各ノードに割り当てられる。

【００３９】そして、センタ１０からユーザ端末１２へ至るツリー経路上に存在したノードの固有番号ＮｉｊとマスタキーデータＫｉｊが調べられ、ノード固有番号ＮｉｊとマスタキーデータＫｉｊ（の並び）で示される各経路が該当のユーザ端末１２に定義される。

【００４０】図４においては、最下位のレイヤ３に配置されている第４ノードのユーザ端末１２にノード番号Ｎ３３，Ｎ２１，Ｎ１０，Ｎ００とマスタキーデータＫ３３、Ｋ２１、Ｋ１０およびＫ００が定義される。

【００４１】ただし、マスタキーデータＫｉｊは乱数を発生させることにより得られており、ノード固有番号Ｎｉｊ，マスタキーデータＫｉｊは該当のユーザ端末１２へ秘密裏に配布される。

【００４２】ここで、ユーザ端末１２が配置された最下位のレイヤより上位側のレイヤに属するノード番号Ｎｉｊの指定で、枝分岐数のユーザ端末１２を指定できる。例えば図４においてノードＮ２１を指定することでノード番号Ｎ３２、Ｎ３３を指定できる。

【００４３】したがって、センタ１０の最上位レイヤに近いレイヤのノード番号Ｎｉｊを指定することにより、そのノードから分岐した経路の先端に配置されているユーザ端末１２の全てを一括してグループ指定することが可能となる。

【００４４】複数のユーザ端末１２をメンバとするグループへセンタ１０より暗号化されたデータを同報するグループ送信に際しては、グループメンバのユーザ端末１２をより多くグループ化できるように、ツリー上位側となるノードの位置と数が算出されてそれらノードの固有番号が指定され、指定された固有番号が示すノードのマスタキーデータでセッションキーのデータが暗号化される。

【００４５】このセッションキーのデータも乱数を発生させることにより得られており、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２のグループへ同報送信すべきデータはセッションキーデータで暗号化され、指定されたノード固有番号ともにセンタ１０からネットワーク１４へ送出される。

【００４６】また各ユーザ端末１２では、ネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め秘密配布された自端末１２のノード固有番号との突き合わせで、自端末１２が同報送信先となる端末グループのメンバであるか否かが判定される。

【００４７】このときに自端末１２が同報送信先となる端末グループのメンバであることが確認されると、ネットワーク１４から受け取ったセッションキーデータがセンタ１０側から予め秘密配布された自端末１２のマスタキーデータで復号され、同ネットワーク１４から受け取った同報送信データが復号後のセッションキーデータを用いて復号される。

【００４８】／＊　第３発明　第４発明　＊／

これらの発明においてもツリー構造を用いたキー配布が行なわれる。ただし、特開平２－３０１２４０などで示される方式が適用される。

【００４９】センタ１０において、十分に大きな一対の素数ｐ，ｑ（ＳＲＡ暗号システムの意味で大きな良い素数とすることが好ましい）と両素数の乗算結果ｎ＝ｐ＊

19

qと両素数から各々定められた一対の数（p－1，q－1）の最小公倍数Lとが予め用意される。

【0050】そしてツリーが生成されると、第3発明では最小公倍数Lと互いに素となる乱数のマスタキーデータ（乱数を発生させて最小公倍数Lと互いに素となるか否かを調べ、素の場合にはこれを採用し、素でない場合にはまた乱数を発生させて最小公倍数Lと互いに素となるか否かを調べる）と固有の番号とが、センタ10から各ユーザ端末12へ至るツリー中の経路上に存在した各ノードへ、割り付けられる。

【0051】第4発明では、素数発生回路などの利用により、最小公倍数Lと互いに素となる数が直接生成され、乱数が最小公倍数Lと互いに素であるかどうかを調べる処理が省略される。

【0052】各ユーザ端末12についてマスタキーデータと固有番号とが定義されると、最小公倍数Lと互いに素となるパスワード，該当のマスタキーデータ，最小公倍数L，乗算結果nにより定まるキー生成データを、指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末12について作成する処理が行なわれる。

【0053】例えば、全てのノードについて　Ｋｌｊ＊（1／Ｋｌｊ）＝ｍｏｄ　Ｌ　となる1／Ｋｌｊを計算し、ユーザ端末12のパスワードＰＷｓ（ｓ＝0，1，・・・，ｔ－1）を入力し、パスワードＰＷｓが最小公倍数Lと互いに素か否かを検査し、素の場合にはそのパスワードを用いてキー生成データを作成し、素でない場合にはパスワードＰＷｓを再度入力する処理が行なわれる。

【0054】各ユーザ端末12のキー生成データＺｓ（ｓ＝0，1，・・・，ｔ－1）は図5のようにして算出でき（公開鍵：マスタキー），該当のキー生成データＺｓ（ｓ＝0，1，・・・ｔ－1），ノード固有番号Ｎ1ｊ及びそのツリー公開鍵のマスタキーデータＫｌｊはセンタ10から各ユーザ端末12へ配布される。

【0055】図6（A）ではユーザ端末12の数が8の場合におけるツリーとキー生成データが対応して示されており、ノード固有番号Ｎ32のユーザ端末12にはノード固有番号（Ｎ32，Ｎ21，Ｎ10，Ｎ00），マ＊

$$KGk_j = Z_j ** (PW_j * K_{k-1_j} * K_{k-2_j} * \cdots * K_{r_j}) \bmod n$$

$$= C ** (1/(K_{0j} * \cdots * K_{kj})) \bmod n$$

のように、パスワードをキー生成データＺｌｊにべき乗してから下位側レイヤにおけるノードのキーデータＫｉｊ（ｉ＝k＋1，・・・，r）を巾乗することで、キー暗号化キーデータＫＧｋｊを作成できる。図6（A）の場合，ノード固有番号32のユーザ端末12は同図（B）のキー暗号化キーデータ（マスタキー）を作成できる。

【0063】キー暗号化キーデータが作成されると、ネ

20

＊スタキーデータ（Ｋ32，Ｋ21，Ｋ10，Ｋ00），キー生成データ（Ｚ32）が配布される。

【0056】グループ送信の開始時にノード固有番号が指定されると、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと乗算結果nとにより定まるキー暗号化キーデータが作成される。

【0057】例えばノード固有番号Ｎｋｊの場合，　ＫＧｋｊ　＝　Ｃ＊＊（1／（Ｋ0ｊ＊Ｋ1ｊ，・・・，＊Ｋｋｊ））　ｍｏｄ　ｎ　のように、キーデータＫｉｊ（ｉ＝0，1，・・・ｋ）と対応のキーデータ1／Ｋｉｊ（ｉ＝0，1，・・・ｋ）を値Ｃ（図5参照）に巾乗することで、キー暗号化キーデータＫＧｋｊを作成できる。

【0058】キー暗号化キーデータが作成されると、乱数を発生させることによってセッションキーデータが生成され、このセッションキーデータがキー暗号化キーデータで暗号化される。

【0059】さらに、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12へ同報すべきデータをセッションキーデータで暗号化され、指定されたノード固有番号，暗号化されたセッションキーデータ，暗号化されたデータがネットワーク14へ送出される。

【0060】各ユーザ端末12においては、ネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とが突き合わされ、自端末12が同報送信先となる端末グループのメンバであるか否かが判定される。

【0061】そして、自端末12が同報送信先となる端末グループのメンバであることが確認されると、自端末12のパスワード（パスワードは各ユーザが所持する），センタ10側から予め配布された自端末12のマスタキーデータ及びキー生成データ（多くの場合、キー生成データは磁気カードやＩＣカードに書き込まれる）を用いてキー暗号化キーデータが作成される。

【0062】例えばノード固有番号Ｎｋｊのユーザ端末の場合，

ネットワーク14から受け取ったセッションキーデータがこのキー暗号化キーデータを用いて復号され、ネットワーク14から受け取った同報送信データが復号後のセッションキーデータで復号される。

【0064】／＊　第5発明　第6発明　第7発明　＊／

これらの発明においても、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の

最小公倍数とが予め用意される。ただし、センタ１０と全てのユーザ端末１２とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーが生成される。

【００６５】例えば、最下位レイヤの上位側となるレイヤのノード数がより上位側となるレイヤの２倍に設定された場合で、ユーザ端末１２の数が８とされたときには、図７に示されるツリーが生成される。

【００６６】そして、最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とがセンタ１０から各ユーザ端末１２へ至るツリー中の経路上に存在した各ノードへ割り付けられ、各ユーザ端末１２についてセンタ１０から自端末１２へ至るツリー中の経路上に存在した全ノードのマスタキーデータと固有番号とが定義されると、上位側のノード同一でデータを同報すべきグループのメンバとなるユーザ端末１２についてグループキーデータＫＫｉｊ（ｉ：最下位レイヤの上位側となるレイヤにおけるノードの通し番号，ｊ：グループ内の通し番号）が定義される。

【００６７】図８では最下位レイヤにおけるユーザ端末１２の数が８とされた場合のユーザグループ化作用が説明されており、同図（Ａ）では２ユーザがグループ化され、同図（Ｂ）では３ユーザがグループ化される。

【００６８】以上の定義が行なわれると、最小公倍数と互いに素となるパスワード，該当のマスタキーデータ，最小公倍数，乗算結果，グループキーデータにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末１２について作成する処理，指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段７０が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する処理が行なわれる。

【００６９】例えば、　Ｋｉｊ＊（１／Ｋｉｊ）　＝　１　ｍｏｄ　Ｌ　及び　ＫＫｉｊ＊（１／ＫＫｉｊ）　＝　１　ｍｏｄ　Ｌ　となるデータＫｉｊ，ＫＫｉｊを計算してから，各ユーザのパスワードＰＷｓ（ｓ＝０，１，・・・，ｔ－１）を入力して最小公倍数Ｌと互いに素となるか否かを検査し、素の場合はそのパスワードを用いてキー生成データＺｓを図９のようにして作成し、素とならない場合は、パスワードを再び入力する処理が行なわれる。

【００７０】各ユーザ端末１２にはノード番号，マスタキーデータ，グループキーデータ及びキー生成データが配布され、例えば、図７（Ａ）におけるノード固有番号２２のユーザ端末１２にはノード固有番号（Ｎ００，Ｎ１０，Ｎ２２，Ｎ２０，Ｎ２１，Ｎ２３），キーデータ（Ｋ００，Ｋ１０，Ｋ２２），（ＫＫ０２，ＫＫ０３，ＫＫ０４，ＫＫ０６，ＫＫ０７，ＫＫ０８），キー生成データ（Ｚ３２）が配布される。

【００７１】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータが暗号化され、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末１２へ同報すべきデータがセッションキーデータで暗号化されると、指定されたノード固有番号，暗号化されたセッションキーデータ，暗号化されたデータがネットワーク１４へ送出される。

【００７２】また各ユーザ端末１２では、ネットワーク１４から受け取ったノード固有番号とセンタ１０側から予め配布された自端末１２のノード固有番号とを突き合せることにより自端末１２が同報送信先となる端末グループのメンバであるか否かが判定され、グループメンバであることが確認されると、自端末１２のパスワードとセンタ１０側から予め配布された自端末１２のマスタキーデータ，キー生成データ及びグループキーデータとを用いてキー暗号化キーデータが作成される。

【００７３】例えば、受信したノード固有番号が最下位レイヤでない場合、あるいは、受信したノード固有番号が最下位レイヤであるものの、受信したノード固有番号が示す最下位レイヤのユーザ端末１２がグループ化されていない場合には、図１０（Ａ）で示される内容の演算が行なわれてキー暗号化キーデータＫＧｋｊが作成される。

【００７４】これに対し、最下位レイヤのユーザ端末１２がグループ化されており、そのグループに自端末１２が含まれている場合には、図１０（Ｂ）で示される内容の演算が行なわれ、キー暗号化キーデータＫＧｋｊが作成される（そのグループに割り当てられたグループキーデータをＫＫｊｃで示す）。図６のノード識別番号Ｎ２２で示されるユーザ端末１２は、図１０（Ｃ）のようにしてキー暗号化キーデータを作成できる。

【００７５】そして、ネットワーク１４から受け取ったセッションキーデータが生成されたキー暗号化キーデータで復号されると、同ネットワーク１４から受け取ったデータが復号される。

【００７６】なお、ツリーの各レイヤにおける分岐数を３以上に設定できる。また、素数発生回路を設け、乱数が最小公倍数Ｌと互いに素であるか否かを調べる処理を省略することも可能である。

【００７７】

【実施例】図１１，図１２では、第１実施例（第１発明及び第２発明に対応）におけるセンタ１０，ユーザ端末１２の構成が各々説明されている。

【００７８】図１１のセンタ１０は、秘密鍵ファイル装置１００，制御回路１０２，データファイル装置１０４，秘密鍵生成起動回路１０６，グループ通信起動回路１０８，乱数発生回路１１０，暗号回路１１２，１１４，鍵選択回路１１６，多重化装置１１８，同報通信装置１２０で構成されている。

【００７９】そのセンタ１０の制御回路１０２から秘密鍵作成命令が送出されると、秘密鍵生成起動回路１０６が起動されてツリーが作成され、ノード識別番号がグループ通信起動回路１０８に格納される。

【００８０】また乱数発生回路１１０も起動されてその乱数がマスタキーのデータとされ、各ユーザ端末１２に関するこのマスタキーのデータとノード固有番号の定義内容が秘密鍵ファイル装置１００に格納される。以上のようにして得られたノード識別番号，マスタキーデータは該当のユーザ端末１２へ秘密鍵としてツリー構造に従い秘密配布される。

【００８１】グループ送信の開始時には、グループ送信の開始命令とグループメンバのユーザ端末１２を特定するデータとが制御回路１０２からグループ通信起動回路１０８に与えられ、グループ通信起動回路１０８でグループ鍵の配送モードが選択される。

【００８２】グループ鍵配送モードの動作がグループ通信起動回路１０８で開始されると、グループメンバのユーザ端末１２のみが自己より下位側のレイヤに存在するノードの固有番号（節点情報）が特定される。

【００８３】このノード固有番号はグループ通信起動回路１０８から鍵選択回路１１６に送られて秘密鍵ファイル装置１００の参照に使用され、その結果、該当のマスタキーデータ（秘密鍵）が秘密鍵ファイル装置１００から取り出され、鍵選択回路１１６から暗号回路１１２に与えられる。

【００８４】一方、グループ通信起動回路１０８により乱数発生回路１１０が起動されて乱数のセッションキーデータが生成され、そのセッションキーデータも暗号回路１１２に与えられる。

【００８５】暗号回路１１２ではマスタキーデータによりセッションキーデータが暗号化され（暗号化セッション鍵），また、暗号回路１１４ではグループ送信の対象となるデータファイル装置１０４のデータが、暗号化されたセッションキーデータより、暗号化される。

【００８６】多重化装置１１８にはノード識別番号、暗号化されたセッションキーデータ、暗号化された同報送信データが与えられ、それらは多重化装置１１８で多重化されてから同報装置１２０からスター状のネットワーク１４へ送出される。

【００８７】図１２のユーザ端末１２は，信号受信・多重分離装置２００、グループ通信検出回路２０、鍵選択回路２０４、秘密鍵ファイル装置２０６、暗号回路２０８、暗号回路２１０、これらを制御する制御回路２１２，データファイル装置２１４，Ｉ／Ｏ装置２１６で構成されている。

【００８８】なお、配布されたマスタキーデータは秘密鍵ファイル装置２０６に格納され、自端末１２に割り付けられたノード固有番号はグループ通信検出回路２０２と鍵選択回路２０４に格納される。

【００８９】上記のセンタ１０からネットワーク１４へ送出されたノード識別番号、セッションキーデータ、同報送信データは信号受信・多重化分離装置２００で信号受信され、分離される。

【００９０】これらのうち、ノード識別番号はグループ通信検出回路２０２で配布済みのノード識別番号と突き合わされ、その結果から、自端末１２がグループ通信のメンバか否かが調べられる。

【００９１】グループメンバであることが確認される、グループ通信検出回路２０２によって鍵選択回路２０４が起動され、秘密鍵ファイル装置２０６から鍵選択回路２０４へ配布済みのマスタキーデータが取り出される。

【００９２】そのマスタキーデータは暗号回路２０８に与えられ、暗号回路２０８では信号受信・多重化分離装置２００から与えられたセッションキーデータが復号される（マスタキーでセッションキーのロックを解除する）。

【００９３】さらに、セッションキーのデータは暗号回路２０８から暗号回路２１０に与えられ、暗号回路２１０では信号受信・多重化分離装置２００から与えられた同報送信データがセッションキーデータを用いて復号される（セッションキーで受信データのロックを解除する）。

【００９４】暗号回路２１０によって復号された同報送信データは、データファイル装置２１４に格納され、あるいは、Ｉ／Ｏ装置を介して外部へ出力され。したがって、ノード識別番号で指定されたユーザ端末１２のみが、この同報送信データを受信出力できる。

【００９５】以上の本実施例によれば、図１３からも理解されるように、ユーザ端末１２が保管すべき秘密鍵の数をわずかなものに抑制しながら、鍵配送回数の増加を回避することが可能となる。

【００９６】図１４，図１５では、第２実施例（第３発明及び第４発明／第５発明，第６発明及び第７発明に対応）におけるセンタ１０，ユーザ端末１２の構成が説明されている。

【００９７】図１４においてセンタ１０は、秘密鍵ファイル装置１００（素数ｐ，ｑ，最小公倍数Ｌが秘密情報として格納されている），公開鍵ファイル装置１０１（乗算結果ｎが公開情報として格納されている），制御回路１０２，データファイル装置１０４，秘密鍵生成起動回路１０６，グループ通信起動回路１０８，乱数発生回路１１０，暗号回路１１２，１１４，鍵生成回路１１７，多重化装置１１８，同報通信装置１２０で構成されている。

【００９８】制御回路１０２から秘密鍵生成起動回路１０６に秘密鍵の作成命令が送出されると、秘密鍵生成起動回路１０６で図７のツリーが生成される。このツリーはグループ通信起動回路１０８に格納され

る。

【0099】また、乱数発生回路110が起動されてノード固有番号と乱数（マスタキーデータ）とが各ノードに割り付けられ（マスタキーデータは仮割り付けされる）、それらがツリー公開鍵のデータとして鍵生成回路117に与えられる。

【0100】鍵生成回路117では公開鍵のマスタデータが所定の条件を満たしているか否かが検査され（最小公倍数しと互いに素となるか否かの検査）、満たしていない場合には、乱数再発生の指示が乱数発生回路110に与えられる。

【0101】その後、全てのユーザ端末12について公開鍵のマスタデータが得られると、秘密鍵（1／KIJのみ、または、1／KIJ及び1／KKIJ）のデータが生成される。なお、全ユーザ端末12の秘密鍵と公開鍵は秘密鍵ファイル装置101、公開鍵ファイル100に各々格納される。

【0102】さらに各ユーザ端末12のパスワード入力が開始され、パスワードの入力毎に鍵生成データ（キー生成データZs：図5，図9参照）が作成される（パスワードの入力毎にそのパスワードが最小公倍数しと互いに素となるか否かが検査される。また、該当の秘密鍵のデータが存在しているか否かもチェックされる。秘密鍵のデータが存在していた場合で、パスワードが最小公倍数しと互いに素となるときには、そのパスワードを用いてキー生成データが作成される。該当の秘密鍵データが存在していなかった場合、または、パスワードが最小公倍数しと互いに素とならない場合、別のパスワードが再び入力される）。このようにして作成されたキー生成データは該当のユーザ端末12へ公開鍵のデータ（ノード固有番号を含む）とともに配布される。

【0103】全てのユーザ端末12にキー生成データが配布された後に、グループ送信が行なわれる。その際には、制御回路100からグループ送信の起動命令とグループ情報とがグループ通信起動回路108に与えられる。

【0104】グループ通信起動回路108では、同報先となるユーザ端末12のみがツリーの下位側に含まれるノードの固有番号を全て求める処理が行なわれ、これらのノード固有番号は鍵生成回路117に与えられる。

【0105】鍵生成回路117においては、公開鍵ファイル装置101から公開鍵のデータを取り出し、各ノードに対応する鍵暗号化鍵のデータ（キー暗号化キーデータKGkj：図10参照）を生成する処理が行なわれ、鍵生成回路117が生成したキー暗号化キーのデータは暗号回路112に与えられる。

【0106】このときにグループ通信起動回路108で乱数発生回路110も起動され、セッション鍵のデータ（セッションキーデータ）が生成される。そのセッションキーデータは暗号回路112に与えられ、鍵生成回路

117で生成されたキー暗号化キーデータにより暗号化される（暗号化セッションキー）。

【0107】また、乱数のセッションキーデータは暗号回路114にも送付され、データファイル装置104から読み出されたグループ送信用のデータがこのセッションキーデータで暗号化される。

【0108】以上のノード固有番号、暗号化されたセッションキーデータ、暗号化された同報送信データは多重化装置118で多重化されてから、同報装置120よりスター状のネットワーク14へ送出される。

【0109】図14において各ユーザ端末12は、信号受信・多重分離装置200、グループ通信検出回路202，鍵生成回路204，公開鍵ファイル装置207，暗号回路208，暗号回路210，これらを制御する制御回路212，データファイル装置214，I／O装置216で構成されている。

【0110】なお、キー生成データとノード固有番号はグループ通信検出回路202，鍵生成回路204に格納される。また、公開鍵のデータは公開鍵ファイル207に格納される。そして、キー生成データはユーザの所持する磁気カードあるいはICカードに書き込まれる。さらに、パスワードは各ユーザによって管理される。

【0111】センタ10がネットワーク14へ送出したノード固有番号，セッションキーデータ，グループ送信データは信号受信・多重化分離装置200で信号受信され、分離される。

【0112】これらのうち、ノード固有番号（接点情報）はグループ通信検出回路202に与えられ、配布されたノード固有番号との突合せで自端末12がグループ通信のメンバか否かが判定される。

【0113】グループメンバの場合には、グループ通信検出回路202により鍵生成回路204が起動され、鍵生成回路204では公開鍵ファイル装置207の公開鍵データ，配布されたキー生成データ，ユーザから入力されたパスワードを用いてキー暗号化キーデータ（鍵暗号化鍵のデータ）が作成される。

【0114】作成されたキー暗号化キーデータは暗号回路208に与えられる。この暗号回路208には信号受信・多重分離装置200からセッションキーデータ（暗号化されている）が与えられ、そのセッションキーデータはキー暗号化キーデータを用いて復号される。

【0115】そして、復号されたセッションキーデータは、暗号回路210に与えられる。暗号回路210には信号受信・多重分離装置200からグループ通信データ（暗号化されている）が与えられ、このグループ送信データは暗号回路208から与えられたセッションキーデータを用いて復号される。

【0116】このようにして暗号回路210で復号されたグループ送信データはデータファイル装置214に格納され、あるいは、I／O装置216を介して外部へ出

27

力される。

【0117】図16（A）では第3発明，第4発明が適用されたときに鍵生成回路204で行なわれる処理の手順がフローチャートを用いて説明されており、また、同図（B）では第5発明，第6発明，第7発明が適用されたときの処理手順が説明されている。

【0118】図16（A），（B）において、センタ10から受信したノード固有番号，配布されたキー生成データ，ユーザ入力のパスワード，公開ファイル装置207のノード固有番号及びマスタキーデータが順に入力される（ステップ1600，1602，1604，1606）。

【0119】そして第3発明，第4発明が適用されたときには図17の処理手順でキー暗号化キーデータが作成される（ステップ1700）。また、第5発明，第6発明，第7発明が適用されたときには最下位のレイヤ内でユーザ端末12をグループ化しているか否かが判断され（ステップ1608）、その判断結果に応じ、図18あるいは図19の処理手順で、キー暗号化キーデータが作成される（ステップ1800，1900）。

【0120】図17においては、キー作成データにマスタキーデータを巾乗する処理（ステップ1702）と、キー作成データにパスワードを巾乗する処理（ステップ1704）とが行なわれる。

【0121】図18の処理は最下位のレイヤ内でユーザ端末12をグループ化しているときに行なわれ、最初にキー作成データへグループキーデータが巾乗され（ステップ1802）、次に、キー作成データへパスワードが巾乗される（ステップ1704）。

【0122】図19の処理は最下位のレイヤ内でユーザ端末12をグループ化していないときに行なわれ、最初に、キー作成データへグループキーデータが巾乗され（ステップ1902）、次に、キー作成データへマスタキーデータが巾乗され（ステップ1904）、最後に、キー作成データへパスワードが巾乗される（ステップ1906）。

【0123】以上の本実施例によれば、図13からも理解されるように、第1実施例に比してユーザ端末12側における秘密鍵の保管数を削減（第3発明，第4発明の適用時）し、あるいは、公開鍵保管数のわずかな増加と引き換えに鍵配送数を大幅に削減（第5発明，第6発明，第7発明の適用時）することが可能となる。

【0124】なお、乱数発生回路110に代えて素数発生回路を設け、鍵生成回路117の処理を簡便化することも可能であり、また、各レイヤの分岐数を3以上として鍵配送数を削減することも好適である。

【0125】

【発明の効果】以上説明したように本発明によれば、センタから各ユーザ端末に至るツリー構造の採用で、鍵配送の所要時間を短縮することが可能となり、また、各ユーザ端末で保管される秘密鍵の数を削減することも可能となる。

28

【図面の簡単な説明】

【図1】第1発明及び第2発明の原理説明図である。

【図2】第3発明及び第4発明の原理説明図である。

【図3】第5発明，第6発明及び第7発明の原理説明図である。

【図4】バイナリツリーの説明図である。

【図5】キー生成データを作成する処理の内容説明図である。

【図6】第3発明及び第4発明の作用説明図である。

【図7】第5発明，第6発明及び第7発明におけるツリー及びキー生成データの説明図である。

【図8】第5発明，第6発明及び第7発明における最下位レイヤのユーザグループ化作用説明図である。

【図9】第5発明，第6発明及び第7発明におけるキー生成データの作成作用説明図である。

【図10】第5発明，第6発明及び第7発明におけるユーザ端末のキー暗号化キー作成作用説明図である。

【図11】第1実施例におけるセンタの構成説明図である。

【図12】第1実施例におけるユーザ端末の構成説明図である。

【図13】発明の効果説明図である。

【図14】第2実施例におけるセンタの構成説明図である。

【図15】第2実施例におけるユーザ端末の構成説明図である。

【図16】第2実施例におけるユーザ端末で行なわれる処理の手順を説明するフローチャートである。

【図17】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

【図18】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

【図19】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

【符号の説明】

10　センタ
12　ユーザ端末
14　ネットワーク
100　秘密鍵ファイル装置
101　公開鍵ファイル装置
102　制御回路
104　データファイル装置
106　秘密鍵生成起動回路
108　グループ通信起動回路
110　乱数発生回路
112，114　暗号回路
116　鍵選択回路
117　鍵生成回路

29

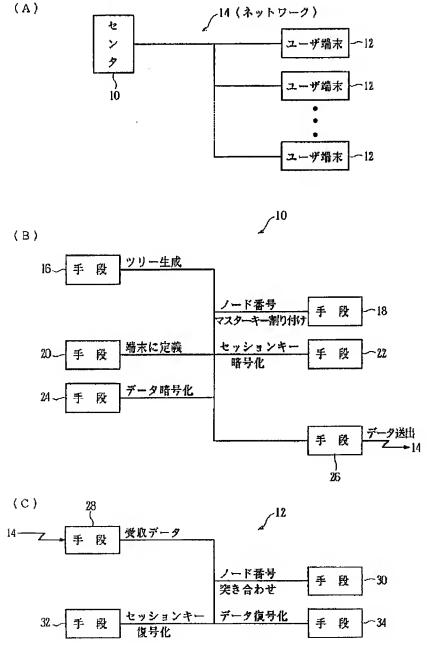
118	多重化装置
120	同報装置
200	信号受信・多重分離装置
202	グループ通信検出回路
204	鍵選択回路
206	秘密鍵ファイル装置

30

207	公開鍵ファイル装置
208，210	暗号回路
212	制御回路
214	データファイル装置
216	Ｉ／Ｏ装置

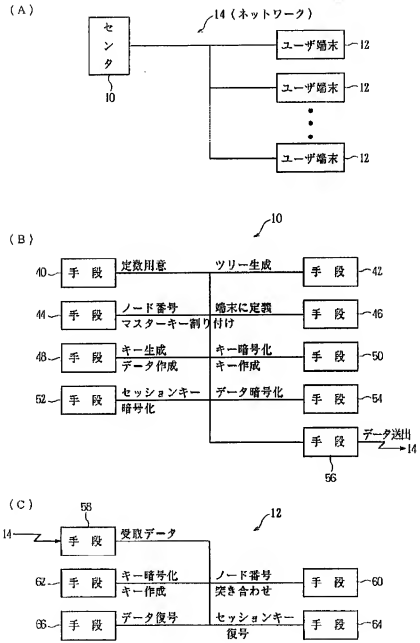
【図1】

第1発明及び第2発明の原理説明図



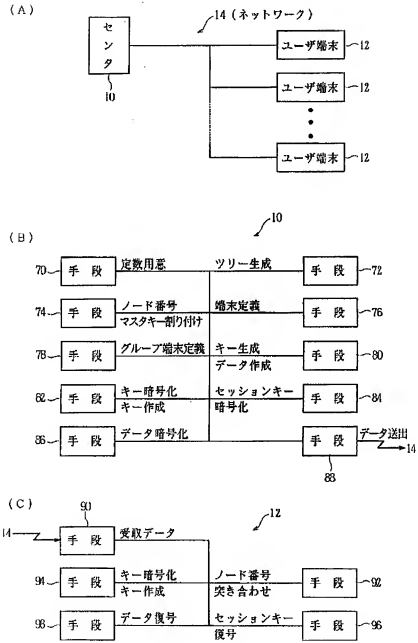
【図2】

第3発明及び第4発明の原理説明図



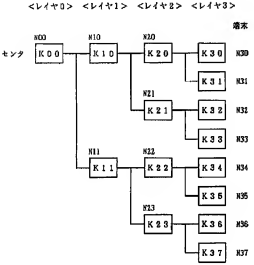
【図3】

第5発明，第6発明及び第7発明の原理説明図



【図４】

バイナリツリーの説明図



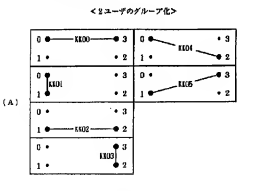
【図５】

鍵生成データを作成する処理の内容説明図

Zs=　C**(1／(PWs*Ks))　mod　n
　C　：センタのＩＤ情報，有効期間等
　Ks　：ユーザsに割当られた公開鍵の集合の積
　　Ks　=　Ｉ Ｉ　Kij
　　{Ｋｉｊ｝∈　Usの内容説明図

【図８】

第５発明，第６発明及び第７発明における再下位レイヤのユーザグループ化作用説明図



【図９】

第５発明，第６発明及び第７発明におけるキー生成データの作成作用説明図

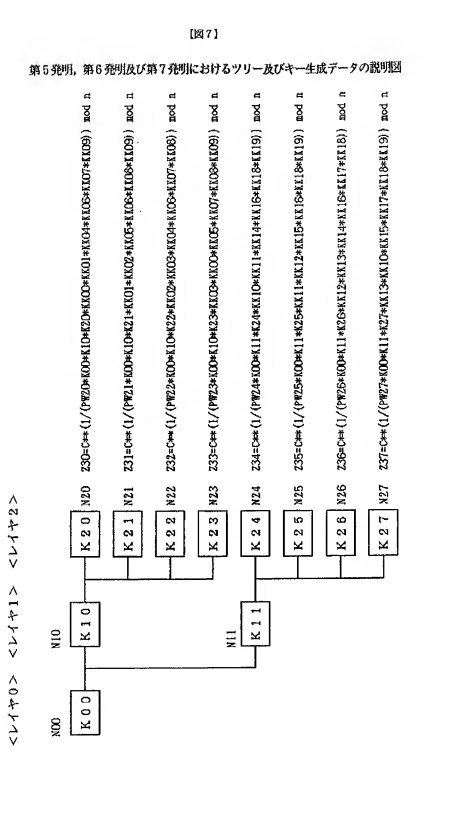
Zs=　C**(1／(PWs*Xs*KKs))　mod　n
　C　：センタのＩＤ情報，有効期間等
　Ks　：ユーザsに割当られたツリー公開鍵の集合の積
　　Ks　=　Ｉ Ｉ　Kij
　　{Ｋｉｊ｝∈　Us
　KKs　：ユーザsに割当られたグループ公開鍵の集合の積
　　KKs　=　Ｊ Ｉ　KKij
　　{ＫＫｉｊ｝∈　Us

【図6】

第3発明及び第4発明の作用説明図

【図7】

第5発明，第6発明及び第7発明におけるツリー及びキー生成データの説明図



【図10】

第5発明，第6発明及び第7発明におけるユーザ端末のキー暗号化キー作成作用説明図

（A）

$$KGKj=Zj^{**}(PWj^{*}K_{k-1\,j}{}^{*}K_{k-2\,j}{}^{*\cdots *}K_{r\,j}{}^{*(\prod_{m=0}^{Ng-1}KKjm)}) \bmod n$$

$$= C^{**}(1/(KOj^{*\cdots *}KKj)) \bmod n$$

（B）

$$KGKj=Zj^{**}(PWj^{*}(\prod_{m=0}^{Ng-1}KKjm)/KKjc * Krj) \bmod n$$

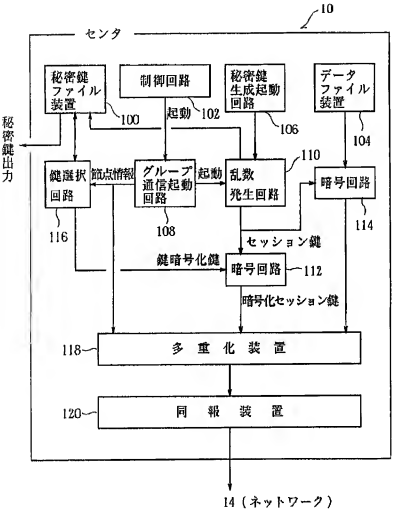
$$= C^{**}(1/(KOj^{*\cdots *}Kr-1\ j^{*}\ Kkjq)) \bmod n$$

（C）

＜指定＞	＜演算内容＞		＜ユーザ端末＞
N00	C**(1/(K00))	mod n	全て
N10	C**(1/(K00*K10))	mod n	N20,N21,N22,N23
N22	C**(1/(K00*K10*K22))	mod n	N22
ｽﾛｰﾁﾞ	C**(1/(K00*K10*KK08))	mod n	N20,N21,N22
ﾆｭｰﾁﾞ	C**(1/(K00*K10*KK04))	mod n	N20,N22

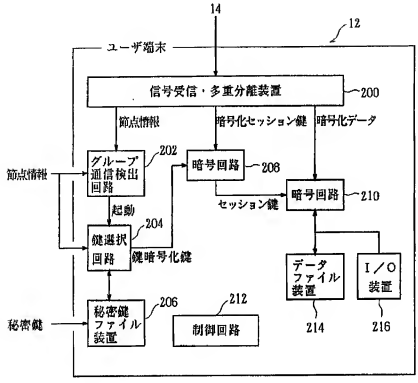
【図１１】

第１実施例におけるセンタの構成説明図



【図12】

第1実施例におけるユーザ端末の構成説明図



【図13】

発明の効果説明図

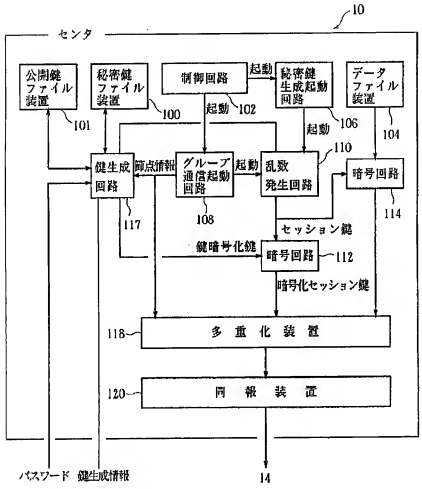
＜ユーザ端末の総数：１２８＞

方　式	センタ側		ユーザ側		鍵配送数			
	秘密鍵数	公開鍵数	秘密鍵数	公開鍵数	Ng=32	Ng=64	Ng=96	Ng=127
通信毎全配布	128		128		32	64	96	127
全鍵保管方式	2**128-1		2**127-1		0	0	0	0
第1及び第2発明	128		128		32*	64*	64*	7*
第3及び第4発明	254	254	1	8	32*	64*	64*	7*
第5，第6及び第7発明（1ツリーグループ）	158 3952	158 3952	1	5 247	16*	16*	16*	5*

Ng：グループ内ユーザ数
＊：最悪値
1：最終点での分岐を８とする

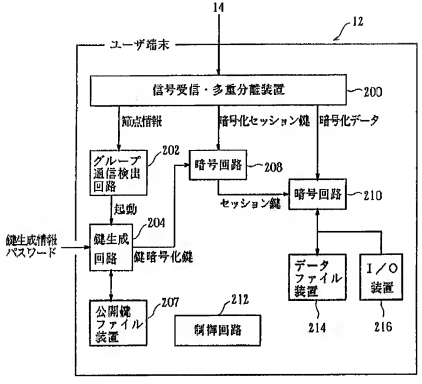
【図14】

第2実施例におけるセンタの構成説明図



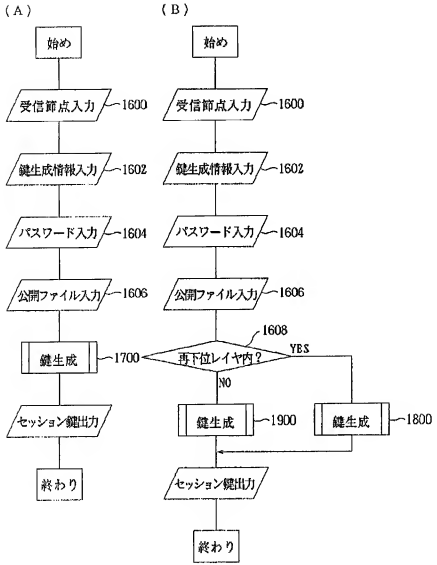
【図15】

第2実施例におけるユーザ端末の構成説明図



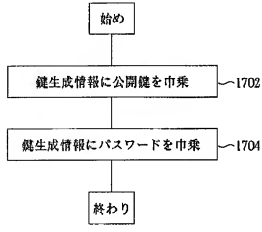
【図16】

第2実施例におけるユーザ端末の行われる処理の手順を説明するフローチャート



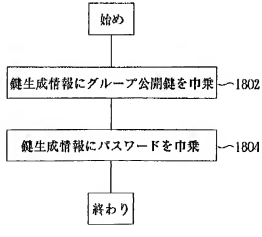
【図17】

第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャート



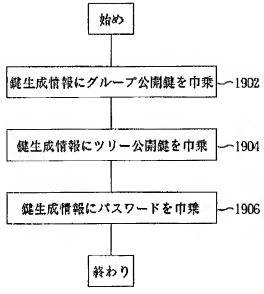
【図18】

第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャート



【図19】

第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャート



フロントページの続き

(51)Int.Cl.⁵	識別記号	庁内整理番号	FI	技術表示箇所
H04L 9/06				
9/14				